APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,847	01/19/2001	Jose C. Brustoloni	Brustoloni 8-5	9246

46363   7590   08/29/2005

MOSER, PATTERSON & SHERIDAN, LLP/
LUCENT TECHNOLOGIES, INC
595 SHREWSBURY AVENUE
SHREWSBURY, NJ 07702

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _13 June 2005_ .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-12 and 14-56_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-12 and 14-56_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _19 January 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____ .

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 3/9/2005 has been entered.

Response to Arguments

2.   In response to communications filed on 6/13/2005, applicant has amended claims 1, 2,

and 53; and has cancelled claim 13. The following claims 1-12 and 14-56 are presented for

examination.

3.   Applicant's remarks, pages 9-14, filed on 6/13/2005, with respect to the rejection of

claims 1 and 53 have been fully considered, but they are not persuasive. Applicant argues that

the cited references do not teach "wherein a service provider that provides the client access

obtains access services from another service provider" as recited in amended claims 1 and 53.

Examiner respectfully disagrees. Van Horne discloses (column 9, lines 12-33) a plurality of

access ports connected via a LAN to server 110 (that meets the recitation of micro service

provider), the server is connected to a router via a communication interface, the router transmits

and receives information to and from the ECN (a second point of service associated with the

service provider), column 6, lines 35-65 describe the ECN as including Internet, on-line services,

dial up computer servers, WAN, ... ECN are accessed by means of ISP, OSP, computer servers,

WAN servers, etc.; the ECN also meets the recitation of another service provider. Therefore, the

reference clearly discloses "wherein a service provider that provides the client access obtains

access services from another service provider". Van Horne further discloses in another

embodiment the server 110 using a T1, ADSL or other high speed transmission line to

communicate with the ECN and using a second different interface to communicate with the

client (column 7, line 40 through column 8, line 18). As mentioned in applicant's argument,

applicant's disclosure (pages 4, lines 16-20 and page 6, lines 21-27) discloses a server (micro

service provider) comprising a LAN and an access link (DSL, cable or T1) to a conventional SP

POP, a router connects the LAN to the conventional service provider SP POP. Applicant has

amended the independent claims by incorporating the limitation of claim 13. Applicant has still

not overcome the combined references. For at least the reasons mentioned above in the last

office action examiner will maintain the rejection. In addition, Garrett discloses secure tunnel

connection between the client devices and the service provider and also discloses two points of

access: a bridge LAN connected to service providers (see page 3, paragraphs 0022-0026).

Therefore, claims 1-12 and 14-56 remain rejected under 35 USC 103 in view of Van Horne,

Garrett, and Mansey.

Claim Objections

4.   **Claim 1** is objected to because of the following informalities: "establishing a secure

tunnel between the service provider" should be --a-- service provider. Appropriate correction is

required to avoid rendering the claim indefinite.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or

described as set forth in section 102 of this title, if the differences between the subject matter

sought to be patented and the prior art are such that the subject matter as a whole would have

been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which

the invention was made.

5.1   **Claims 1-12, 14-56** are rejected under 35 U.S.C. 103(a) as being unpatentable over US

Patent 6,128,601 to **Van Horne et al.** in view of US Patent Publication US 2002/0019875 to

Garrett et al. and in view of US Patent 6,023,499 to **Mansey et al..**

5.2   **As per claims 1, 2, 50, 53, Van Horne et al.** substantially teaches a method and

apparatus for providing client access to the Internet or other network, comprising: offering, at a

point of service, a Local Area Network (LAN) connected to the Internet or other network, for

example (see figure 5 and column 8, lines 4-39 and lines 50-65); connecting at least one client

computer to said LAN, for example (see column 9, lines 12-32; column 7, lines 40-67; and figure

5); configuring networking parameters of each of said at least one client computer, for example

(see column 4, lines 38-65 and column 10, lines 37-67); establishing a secure connection

between the service provider and each of said at least one client computer, such that the service

provider provides Internet or other network service through the secure connection to only each

one of said at least one client computer, for example (see column 9, lines 12-32 and column 10,

lines 27-67; column 14, line 35 through column line 15, line 25); and providing the Internet or

other network service at the first point of service to each one of the at least one client computer

in accordance with the network usage terms and prices via a second point of service associated

with the service provider, for example (see column 9, lines 12-32; column 7, lines 40-67 and

column 4, lines 10-65). (See also columns 17 et seq. for more details on network usage terms

and prices). **Van Horne** discloses (column 9, lines 12-33) a plurality of access ports connected

via a LAN to server 110 (that meets the recitation of micro service provider), the server is

connected to a router via a communication interface, the router transmits and receives

information to and from the ECN (a second point of service associated with the service

provider), column 6, lines 35-65 describe the ECN as including Internet, on-line services, dial up

computer servers, WAN, ... ECN are accessed by means of ISP, OSP, computer servers , WAN

servers, etc.; the ECN also meets the recitation of another service provider. See also column 14,

line 35 through column line 15, line 25). Therefore, the reference clearly discloses "wherein a

service provider that provides the client access obtains access services from another service

provider". **Van Horne** further discloses in another embodiment the server 110 using a T1,

ADSL or other high speed transmission line to communicate with the ECN and using a second

different interface to communicate with the client (column 7, line 40 through column 8, line 18).

Van Horne et al. discloses establishing a secure connection between the client and the service

provider at the first point of access, but does not explicitly state using "a secure tunnel", which is

well known in the art, or exchanging authentication certificate as recited in claim 53 which is

notoriously well known. **Garrett et al.** in an analogous art teaches establishing a secure tunnel

between the service provider and each of said at least one client computer, such that the service

provider provides Internet or other network service through the secure tunnel to only each one of

said at least one client computer. In one embodiment, a VLAN is used in order to maintain

control and isolate traffic to individual services/service providers, for example (see page 2,

paragraph 0019 and page 3, paragraphs 0021-0026). **Garrett et al.** also discloses to implement

the invention using a number of different communication protocols, such Internet protocols are

very well known in the art as disclosed, for example (see page 1, column 0010). For instance

RFC 1426 and 1826 discuss Certificate Key-Based Management, exchanging authentication

certificates, IP authentication header, packet encryption, and Certificate Authority, etc.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention

was made to modify the method of **Van Horne et al.** to establish a secure tunnel with said

service provider by exchanging authentication certificate with the first access point of said

service provider, in order to provide Internet or other network service through the secure tunnel

to only each one of said at least one client computer by encapsulating traffic; maintain control

and provide initialization and authentication procedures between the service provider and the

client as taught by **Garrett et al.**. This modification would have been obvious because one

skilled in the art would have been motivated by the suggestions provided by **Garrett et al.** so as

to provide Internet or other network service through the secure tunnel to only each one of said at

least one client computer by encapsulating traffic; maintain control and provide initialization and

authentication procedures between the service provider and the client, for example (see page 1,

column 0010 and page 3, paragraph 0019).

Van Horne et al. discloses selecting billing options at the point of service, and also

discloses billing preferences, and network usage terms and prices with each one of said at least

one client computer, for example (see column 4, lines 24-38; see also column18 lines 41 et seq.).

It is obvious to one skilled in the art that the billing options and preferences disclosed by Van

Horne et al. may also imply the selection of term and prices which does not depart from the

spirit and scope of the invention as at the end of the session a display of usage and prices is

shown for example in figure 16. Mansey et al. in an analogous art teaches a method of

monitoring charges associated to any types of communication networks, for example (see

column 3, line 55 through column 4 line 5); negotiating, at the point of service, the network

usage terms and prices with each one of said at least one client computer, for example (see

column 1, line 60 through column 2, line 40) and accessing said Internet via said service provider

according to said negotiated usage terms, for example (see column 5, lines 45-65). Mansey et

al. further discloses that the invention is advantageous as it provides continuous tracking and

displaying of the running costs during usage of the service and allows the user to define a

maximum cost limit for a particular use of the service and accessing said Internet via said service

provider according to said negotiated usage terms, for example (see column 2, lines 21-32).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention

was made to modify the method of Van Horne et al. to negotiate, at the point of service, the

network usage terms and prices with each one of said at least one client computer as taught by

Mansey et al.. This modification would have been obvious because one skilled in the art would

have been motivated by the suggestions provided by **Mansey et al.** so as to provide continuous

tracking and displaying of the running costs during usage of the service and allows the user to

define a maximum cost limit for a particular use of the service, for example (see column 2, lines

21-32).

As per claims 3, 4, 6, 22, 30, and 56, Mansey et al. discloses the limitation of placing a

contract for a particular usage that meets the recitation of wherein the contract does not depend

on a previous or subsequent relationship between client and service provider. **Mansey et al. also**

discloses a user of a client computer may monitor and control of client usage, for example (see

column 2, lines 1-5 and lines 27-31). Therefore, these claims are rejected on the same rationale

as the rejection of claims 1 and 53 above.

As per claim 5 and 55, Van Horne et al. discloses the limitation of wherein the client's

usage is measured by bytes or packets transmitted or received, or by the contract's active or

elapsed time, for example (see column 19, line 59 through column 20, line 40; and column 21,

lines 1-15).

As per claims 7, Van Horne et al. discloses the limitation of wherein the client may

choose a hard usage limit, such that the service provider terminates the contract when the hard

limit is reached, for example (see column 17, lines 12-36).

As per claim 8, Van Horne et al. discloses the limitation of where, after receiving a deposit, the service provider sends to the client computer a receipt that the client computer may use to recover from a client computer or service provider failure, obtaining access again on the same contract, for example (see column 17, line 4 through column 18, line 12).

As per claim 9, Van Horne et al. discloses the limitation of wherein the receipt contains all the information required for recovery, for example (see column 17, line 4 through column 18, line 12).

As per claim 10, Van Horne et al. discloses the limitation of wherein the contract is established and the client may monitor and control its usage via a Transport Layer Security protocol or via a Secure Socket Layer connection as discussed above, for example (see columns 16-17) and **Mansey et al.** discloses establishing a contract. Therefore, claim 10 is rejected on the same rationale as the rejection of claims 1 and 53 above.

As per claims 11 and 12, Van Horne et al. discloses the limitation of wherein the service provider owns or rents the premises at the point of access, wherein access is provided in one of an airport, hotel, conference center, or a multi-tenant building for example (see column 4, lines 54-65).

As per claim 14, Van Horne et al. discloses the limitation of wherein a service provider that provides client access is connected to the Internet by one or more Digital Subscriber Lines

(DSL), T1 or other dedicated telephone lines, Integrated Services Digital Network (ISDN) lines,

or cable modems, for example (see column 7, lines 50-65).

As per claims 15 and 17, Garrett et al. discloses the limitation of wherein a service

provider that provides the client access uses Network Address Translation, for example (see page

1, paragraph 0002 and 0010), and wherein the network configuration of client computers is

performed by the Dynamic Host Configuration Protocol, for example (see page 2, paragraph

0019). Therefore, claims 15 and 17 are rejected on the same rationale as the rejection of claims 1

and 53 above.

As per claim 16, Van Horne et al. discloses the limitation of wherein the network

configuration of client computers is automatic, for example (see column 11, lines 32-35).

Claims 18-20 recite authentication of packets between the service provider and the client

and encrypting packets, which was discussed in claims 1 and 23 above. Therefore, claims 18-20

are rejected on the same rationale as the rejection of claims 1 and 53 above.

As per claim 21, Garrett et al. discloses the limitation of wherein the client computer

may choose whether packets sent from or via a service provider to the client computer should be

authenticated, or whether packets sent between the client computer and a service provider should

be encrypted, for example (see page 3, paragraph 0024) and is also well known in the art as

discussed in RFC 1826. Therefore, claim 21 is rejected on the same rationale as the rejection of

claims 1 and 23 above.

As per claims 23 and 24, Mansey et al. discloses the limitation of wherein the client

may choose a soft usage limit, such that the service provider suspends service to the client when

the soft limit is reached and sends a notification to the client, and the client may resume service

and set a new soft limit by sending a message to the service provider, further comprising the

client paying for said Internet or other network service, wherein the payment is offline, for

example (see column 6, lines 5-37). Therefore, claims 23 and 24 are rejected on the same

rationale as the rejection of claims 1 and 53 above.

As per claims 25-29, Van Horne et al. discloses the limitation of wherein payment is by

one or more of the following options: cash, credit card, and debiting from another account and

further comprising the client paying for said Internet or other network service, wherein the

payment is online, for example (see column 13, line 49 through column 14, line 36). It is

obvious that the online payment can be performed by one of the companies eCASH®. SECURE

ELECTRONIC TRANSACTIONS (SET)®, IBM MICROPAYMENTS®, or MILLICENT®.

As per claims 31-32, Van Horne et al. discloses the limitation of wherein the user of the

client computer, before gaining service pays to the service provider a deposit, and, when the user

requests contract termination, the service provider returns to the user the difference between the

deposit and actual usage for example (see column 19, line 59 through column 20, line 40; and

column 21, lines 1-15). It is apparent to one skilled in the art that the service provider returns to

the user the balance, which is the difference between the deposit and actual usage.

As per claims 33-35, Van Horne et al. discloses the limitation of wherein the client

computers are not portable and wherein the client computers are portable, wherein the client

computers are wearable, for example (see column 6, lines 35-65).

As per claims 36-38, Van Horne et al. discloses the limitation of using LAN as

Ethernet, wireless network or any other communication network known in the art (column 7, line

40 through column 8, line 65).

Claims 39-48 and 54 recite standard Internet Protocols well known in the art discussed

above in claim 1. Claims **39-40** are disclosed in claim 1, for example (see **Garrett et al.** page 1,

paragraph 0010). Claims **41-44** recite limitation of using authentication certificate signed by a

certification authority and the limitation of wherein the client computer uses a self-signed

certificate and the certificate includes information of the service providers. **Garrett et al.** also

suggests to implement the invention using a number of different communication protocols, such

Internet protocols are very well known in the art as disclosed, for example (see page 1, column

0010). For instance RFC 1426 and 1826 discuss Certificate Key-Based Management,

exchanging authentication certificates, IP authentication header, packet encryption, and

Certificate Authority, etc. (see RFC documentation provided); For instance, (X.509 architecture)

disclose authentication certificate by a certification authority including the content of a

certificate. As per **claims 45-48**, RFC 1825 also discloses authentication header, ESP, etc. .

Therefore, claims 39-48 and 54 are rejected on the same rationale as the rejection of claims 1 and

53 above.

As per claims 49, 51, and 52, Garrett et al. discloses the limitation of wherein the user

of the client computer does not reveal its identity to the service provider, for example (see page

4, paragraph 0031) and also discloses wherein service provider functionality is implemented by

an integrated router/server or implemented by separate router and server, for example (see page

2, paragraph 0013). Therefore, claims 49, 51, and 52 are rejected on the same rationale as the

rejection of claims 1 and 53 above.

Conclusion

6.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure as the art discloses the use of network address translations in network services and

establishing secure tunnel with service provider. Many of the claimed features , i.e. secure

tunnel with Ipsec, Internet protocol authentication, encryption etc. are disclosed in these

references.

US Patent Publication   US 2002/0026503   Bendinelli et al.

US Patents   6,055,236 Nessett et al,   5,805,803 Birrell et al.

6.21   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The

examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin
Patent Examiner
August 20, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100